(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－66986
（P2001－66986A）
(43)公開日　平成13年３月16日(2001.3.16)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ｂ	５Ｂ０４９
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	Ｚ	５Ｊ１０４
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｋ０３２
9/32			６７５Ａ	５Ｋ０３４
12/40		11/00	３２０	９Ａ００１

審査請求　未請求　請求項の数11　ＯＬ　（全 17 頁）　最終頁に続く

(21)出願番号　特願平11－239205

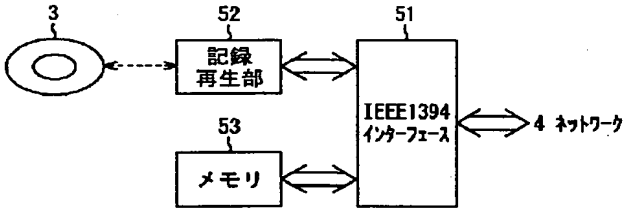
(22)出願日　平成11年８月26日(1999.8.26)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　海老原　宗毅
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　送信装置および方法、受信装置および方法、通信システム、並びにプログラム格納媒体

(57)【要約】
【課題】　不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限する。
【解決手段】　メモリ５３は、コンテンツ管理データのハッシュ値を記憶する。IEEE1394インターフェース５１は、ネットワークを介して接続されているパーソナルコンピュータを認証するとき、パーソナルコンピュータにコンテンツ管理データを送信するとともに、パーソナルコンピュータからコンテンツ管理データのハッシュ値を受信する。IEEE1394インターフェース５１は、パーソナルコンピュータを認証するとき、受信したコンテンツ管理データのハッシュ値と、記憶しているコンテンツ管理データのハッシュ値との一致を判定する。



DVDドライブ 2

【特許請求の範囲】

【請求項１】　第１のデータおよび前記第１のデータの利用の制限を記述する第２のデータが記録されている記録媒体を駆動して、前記第１のデータを受信装置に送信する送信装置において、

前記第２のデータの暗号値を記憶する記憶手段と、

前記受信装置を認証する場合、前記受信装置に前記第２のデータを送信するとともに、前記受信装置から前記第２のデータの暗号値を受信する通信手段と、

前記受信装置を認証する場合、前記通信手段が受信した前記第２のデータの暗号値と、前記記憶手段が記憶している前記第２のデータの暗号値との一致を判定する判定手段とを含むことを特徴とする送信装置。

【請求項２】　前記記憶手段は、認証以外の処理において、前記第２のデータの暗号値の書き込みまたは読み出しを禁止することを特徴とする請求項１に記載の送信装置。

【請求項３】　前記記憶手段は、耐タンパー性を有することを特徴とする請求項１に記載の送信装置。

【請求項４】　第１のデータおよび前記第１のデータの利用の制限を記述する第２のデータが記録されている記録媒体を駆動して、前記第１のデータを受信装置に送信する送信装置の送信方法において、

前記第２のデータの暗号値を記憶する記憶ステップと、

前記受信装置を認証する場合、前記受信装置に前記第２のデータを送信するとともに、前記受信装置から前記第２のデータの暗号値を受信する通信ステップと、

前記受信装置を認証する場合、前記通信ステップの処理で受信した前記第２のデータの暗号値と、前記記憶ステップの処理で記憶している前記第２のデータの暗号値との一致を判定する判定ステップとを含むことを特徴とする送信方法。

【請求項５】　第１のデータおよび前記第１のデータの利用の制限を記述する第２のデータが記録されている記録媒体を駆動して、前記第１のデータを受信装置に送信する送信処理用のプログラムであって、

前記第２のデータの暗号値を記憶する記憶ステップと、

前記受信装置を認証する場合、前記受信装置に前記第２のデータを送信するとともに、前記受信装置から前記第２のデータの暗号値を受信する通信ステップと、

前記受信装置を認証する場合、前記通信ステップの処理で受信した前記第２のデータの暗号値と、前記記憶ステップの処理で記憶している前記第２のデータの暗号値との一致を判定する判定ステップとからなることを特徴とするプログラムを送信装置に実行させるプログラム格納媒体。

【請求項６】　送信装置が送信した第１のデータを受信する受信装置において、

前記送信装置を認証する場合、前記送信装置から第１のデータの利用の制限を記述する第２のデータを受信するとともに、前記送信装置に前記第２のデータの暗号値を送信する通信手段と、

前記送信装置を認証する場合、前記通信手段が受信した第２のデータを基に、前記第２のデータの暗号値を生成する暗号値生成手段とを含むことを特徴とする受信装置。

【請求項７】　所定のビット数の乱数を生成する乱数生成手段を更に含み、前記通信手段は、前記送信装置に、前記乱数生成手段が生成した前記乱数とともに、前記第２のデータの暗号値を送信することを特徴とする請求項６に記載の受信装置。

【請求項８】　前記通信手段が受信した前記第２のデータを基に、前記第１のデータの受信後の前記第１のデータの利用の制限を記述する第３のデータを生成する利用制限データ生成手段を更に含み、

前記暗号値生成手段は、前記利用制限データ生成手段が生成した前記第３のデータの暗号値を更に生成し、

前記通信手段は、前記送信装置に、前記第３のデータの暗号値とともに、前記第２のデータの暗号値を送信することを特徴とする請求項６に記載の受信装置。

【請求項９】　送信装置が送信した第１のデータを受信する受信装置の受信方法において、

前記送信装置を認証する場合、前記送信装置から第１のデータの利用の制限を記述する第２のデータを受信するとともに、前記送信装置に前記第２のデータの暗号値を送信する通信ステップと、

前記送信装置を認証する場合、前記通信ステップの処理で受信した第２のデータを基に、前記第２のデータの暗号値を生成する暗号値生成ステップとを含むことを特徴とする受信方法。

【請求項１０】　送信装置が送信した第１のデータを受信する受信処理用のプログラムであって、

前記送信装置を認証する場合、前記送信装置から第１のデータの利用の制限を記述する第２のデータを受信するとともに、前記送信装置に前記第２のデータの暗号値を送信する通信ステップと、

前記送信装置を認証する場合、前記通信ステップの処理で受信した第２のデータを基に、前記第２のデータの暗号値を生成する暗号値生成ステップとからなることを特徴とするプログラムを受信装置に実行させるプログラム格納媒体。

【請求項１１】　第１のデータおよび前記第１のデータの利用の制限を記述する第２のデータが記録されている記録媒体を駆動して、前記第１のデータを送信する送信装置、および前記第１のデータを受信する受信装置からなる通信システムにおいて、

前記送信装置は、

前記第２のデータの暗号値を記憶する記憶手段と、

前記受信装置を認証する場合、前記受信装置に前記第２のデータを送信するとともに、前記受信装置から前記第

２のデータの暗号値を受信する第１の通信手段と、
前記受信装置を認証する場合、前記第１の通信手段が受信した前記第２のデータの暗号値と、前記記憶手段が記憶している前記第２のデータの暗号値との一致を判定する判定手段とを含み、
前記受信装置は、
前記送信装置を認証する場合、前記送信装置から前記第２のデータを受信するとともに、前記送信装置に前記第２のデータの暗号値を送信する第２の通信手段と、
前記送信装置を認証する場合、前記第２の通信手段が受信した第２のデータを基に、前記第２のデータの暗号値を生成する暗号値生成手段とを含むことを特徴とする通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、送信装置および方法、受信装置および方法、通信システム、並びにプログラム格納媒体に関し、特に、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようにした送信装置および方法、受信装置および方法、通信システム、並びにプログラム格納媒体に関する。

【０００２】

【従来の技術】画像または音声などのコンテンツデータ、またはコンピュータプログラムなどを使用者者に提供する提供者は、これらのコンテンツデータなどが無制限にコピーされて利用されることを防止するため、これらのコンテンツデータなどを予め暗号化して使用者に提供することがある。

【０００３】このような場合において、所定の暗号鍵を有する正当な使用者だけが、暗号化されているコンテンツデータなどを利用できる。

【０００４】また、コンテンツデータなどの不正な利用を、より強力に防止するため、一部の装置は、コンテンツデータなどを再生する装置とコンテンツデータなどを記録している記録媒体を駆動する装置とを相互認証させるなどの方法が採用する。

【０００５】更に、提供者がコンテンツデータなどの利用の回数を制限したいとき、提供者は、コンテンツデータなどとともにコンテンツデータなどの利用の回数を管理するためのデータを記録媒体に記録して、提供する場合がある。この場合、記録媒体を駆動する装置は、記録媒体に記録されているコンテンツデータなどを読み出すとき、コンテンツデータなどの利用の回数を管理するためのデータを基に、コンテンツデータなどを読み出す回数が予め設定されている回数を越えるか否かを判定して、コンテンツデータなどを読み出す回数が予め設定されている回数を越えたとき、コンテンツデータなどの利用を禁止する。

【０００６】

【発明が解決しようとする課題】しかしながら、コンテンツデータなどと共に、利用の回数を管理するためのデータを他の記録媒体にバックアップして、そのコンテンツデータなどを利用した後、バックアップされた利用の回数を管理するためのデータを元の記録媒体に戻せば、利用者は、無制限にコンテンツデータなどを利用することができる。

【０００７】同様に、そのコンテンツデータなどを他の記録媒体に移動するとき、予め、コンテンツデータなどと共に、利用の回数を管理するためのデータを更に他の記録媒体にバックアップして、そのコンテンツデータなどを他の記録媒体に移動した後、更に他の記録媒体からコンテンツデータなどと共に、利用の回数を管理するためのデータを元の記録媒体に戻せば、利用者は、無制限にコンテンツデータなどを複製することができる。

【０００８】コンテンツデータなどの他の記録媒体への移動の処理における、コンテンツデータなどまたは利用の回数を管理するためのデータの削除の処理を妨害しても、同様に、無制限なコンテンツデータなどの複製が可能になり、利用者は、無制限にコンテンツデータなどを利用することができる。

【０００９】本発明はこのような状況に鑑みてなされたものであり、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようにすることを目的とする。

【００１０】

【課題を解決するための手段】請求項１に記載の送信装置は、第２のデータの暗号値を記憶する記憶手段と、受信装置を認証する場合、受信装置に第２のデータを送信するとともに、受信装置から第２のデータの暗号値を受信する通信手段と、受信装置を認証する場合、通信手段が受信した第２のデータの暗号値と、記憶手段が記憶している第２のデータの暗号値との一致を判定する判定手段とを含むことを特徴とする。

【００１１】記憶手段は、認証以外の処理において、第２のデータの暗号値の書き込みまたは読み出しを禁止するようにすることができる。

【００１２】記憶手段は、耐タンパー性を有するようにすることができる。

【００１３】請求項４に記載の送信方法は、第２のデータの暗号値を記憶する記憶ステップと、受信装置を認証する場合、受信装置に第２のデータを送信するとともに、受信装置から第２のデータの暗号値を受信する通信ステップと、受信装置を認証する場合、通信ステップの処理で受信した第２のデータの暗号値と、記憶ステップの処理で記憶している第２のデータの暗号値との一致を判定する判定ステップとを含むことを特徴とする。

【００１４】請求項５に記載のプログラム格納媒体のプログラムは、第２のデータの暗号値の記憶を制御する記憶制御ステップと、受信装置を認証する場合、受信装置

に第２のデータを送信するとともに、受信装置から第２のデータの暗号値を受信する通信ステップと、受信装置を認証する場合、通信ステップの処理で受信した第２のデータの暗号値と、記憶制御ステップの処理で記憶している第２のデータの暗号値との一致を判定する判定ステップとを含むことを特徴とする。

【００１５】請求項６に記載の受信装置は、送信装置を認証する場合、送信装置から第１のデータの利用の制限を記述する第２のデータを受信するとともに、送信装置に第２のデータの暗号値を送信する通信手段と、送信装置を認証する場合、通信手段が受信した第２のデータを基に、第２のデータの暗号値を生成する暗号値生成手段とを含むことを特徴とする。

【００１６】受信装置は、所定のビット数の乱数を生成する乱数生成手段を更に設け、通信手段は、送信装置に、乱数生成手段が生成した乱数とともに、第２のデータの暗号値を送信するようにすることができる。

【００１７】受信装置は、通信手段が受信した第２のデータを基に、第１のデータの受信後の第１のデータの利用の制限を記述する第３のデータを生成する利用制限データ生成手段を更に設け、暗号値生成手段は、利用制限データ生成手段が生成した第３のデータの暗号値を更に生成し、通信手段は、送信装置に、第３のデータの暗号値とともに、第２のデータの暗号値を送信するようにすることができる。

【００１８】請求項９に記載の受信方法は、送信装置を認証する場合、送信装置から第１のデータの利用の制限を記述する第２のデータを受信するとともに、送信装置に第２のデータの暗号値を送信する通信ステップと、送信装置を認証する場合、通信ステップの処理で受信した第２のデータを基に、第２のデータの暗号値を生成する暗号値生成ステップとを含むことを特徴とする。

【００１９】請求項１０に記載のプログラム格納媒体のプログラムは、送信装置を認証する場合、送信装置から第１のデータの利用の制限を記述する第２のデータを受信するとともに、送信装置に第２のデータの暗号値を送信する通信ステップと、送信装置を認証する場合、通信ステップの処理で受信した第２のデータを基に、第２のデータの暗号値を生成する暗号値生成ステップとを含むことを特徴とする。

【００２０】請求項１１に記載の通信システムは、送信装置が、第２のデータの暗号値を記憶する記憶手段と、受信装置を認証する場合、受信装置に第２のデータを送信するとともに、受信装置から第２のデータの暗号値を受信する第１の通信手段と、受信装置を認証する場合、第１の通信手段が受信した第２のデータの暗号値と、記憶手段が記憶している第２のデータの暗号値との一致を判定する判定手段とを含み、受信装置が、送信装置を認証する場合、送信装置から第２のデータを受信するとともに、送信装置に第２のデータの暗号値を送信する第２の通信手段と、送信装置を認証する場合、第２の通信手段が受信した第２のデータを基に、第２のデータの暗号値を生成する暗号値生成手段とを含むことを特徴とする。

【００２１】請求項１に記載の送信装置、請求項４に記載の送信方法、および請求項５に記載のプログラム格納媒体においては、第２のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第２のデータが送信されるとともに、受信装置から第２のデータの暗号値が受信され、受信装置を認証する場合、受信した第２のデータの暗号値と、記憶している第２のデータの暗号値との一致が判定される。

【００２２】請求項６に記載の受信装置、請求項９に記載の受信方法、および請求項１０に記載のプログラム格納媒体においては、送信装置を認証する場合、送信装置から第１のデータの利用の制限を記述する第２のデータが受信されるとともに、送信装置に第２のデータの暗号値が送信され、送信装置を認証する場合、受信した第２のデータを基に、第２のデータの暗号値が生成される。

【００２３】請求項１１に記載の通信システムにおいては、第２のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第２のデータが送信されるとともに、受信装置から第２のデータの暗号値が受信され、受信装置を認証する場合、受信した第２のデータの暗号値と記憶している第２のデータの暗号値との一致が判定され、送信装置を認証する場合、送信装置から第２のデータが受信されるとともに、送信装置に第２のデータの暗号値が送信され、送信装置を認証する場合、受信した第２のデータを基に、第２のデータの暗号値が生成される。

【００２４】

【発明の実施の形態】図１は、本発明に係る記録システムの一実施の形態を示す図である。パーソナルコンピュータ１は、IEEE（Institute of Electrical and Electronic Engineers）1394の規格に基づくネットワーク４を介して、DVD（Digital Versatile Disc）ドライブ２に接続されている。

【００２５】パーソナルコンピュータ１は、DVDドライブ２からの音声または画像（動画像または静止画像）などのデータであるコンテンツデータの供給に先立ち、DVDドライブ２と相互認証する。この相互認証の手続きにおいて、パーソナルコンピュータ１は、ネットワーク４を介して、DVDドライブ２より供給された、コンテンツデータの利用の条件等が記述されているコンテンツ管理データを受信する。パーソナルコンピュータ１は、パーソナルコンピュータ１でのコンテンツデータの利用（コンテンツの再生、またはコンテンツデータのコピーなど）に対応して、コンテンツ管理データを更新する。

【００２６】パーソナルコンピュータ１は、DVDドライブ２より受信したコンテンツ管理データおよび更新した

コンテンツ管理データのそれぞれに、ＭＤ（Message Digest）５などの一方向ハッシュ関数を適用して、受信したコンテンツ管理データおよび更新したコンテンツ管理データのそれぞれの一方向性暗号値であるハッシュ値を求める。

【００２７】受信したコンテンツ管理データのハッシュ値および更新したコンテンツ管理データのハッシュ値は、パーソナルコンピュータ１が生成した乱数と共に、DVDドライブ２に送信される。

【００２８】パーソナルコンピュータ１は、DVDドライブ２と相互認証した後、例えば、DVDドライブ２から供給された音声または画像などのデータであるコンテンツデータ（暗号化されている）およびコンテンツデータを暗号化しているコンテンツ鍵を受信して、コンテンツ鍵でコンテンツデータを復号して、復号したコンテンツデータを再生する。

【００２９】DVDドライブ２は、相互認証の手続きにおいて、DVD３に記録されているコンテンツ管理データを読み出して、ネットワーク４を介して、パーソナルコンピュータ１に送信する。DVDドライブ２は、相互認証の手続きにおいて、パーソナルコンピュータ１から、コンテンツ管理データのハッシュ値、更新されたコンテンツ管理データのハッシュ値、およびパーソナルコンピュータ１が生成した乱数を受信する。

【００３０】DVDドライブ２は、パーソナルコンピュータ１と相互認証した後、装着されているDVD３に記録されている音声または画像などのデータであるコンテンツデータおよびコンテンツ鍵を読み出し、ネットワーク４を介して、パーソナルコンピュータ１に供給する。

【００３１】DVDドライブ２は、後述するメモリに、DVD３に記録されているコンテンツ鍵を暗号化している暗号鍵である保存鍵、およびコンテンツ管理データにハッシュ関数を適用して得られた値であるハッシュ値を記憶している。

【００３２】DVD３は、コンテンツ鍵で暗号化されているコンテンツデータ、コンテンツデータを暗号化している暗号鍵であるコンテンツ鍵、およびコンテンツデータの利用を管理するためのコンテンツ管理データを記録している。

【００３３】DVD３に記録されているコンテンツデータは、共通鍵暗号方式であるDES（DataEncryption Standard）またはIDEA（International Data Encryption Algorithm）などの方式で、コンテンツ鍵で暗号化されている。

【００３４】DVD３に記録されているコンテンツデータは、コンテンツ管理データに基づき、再生の回数、他の記録媒体へのコピー、他の記録媒体への移動が管理され、これらの操作が許可される。

【００３５】コンテンツ管理データは、例えば、コンテンツデータが許可されている利用の形態（例えば、コンテンツの再生、コンテンツデータのコピー、またはコンテンツデータの移動など）を示すデータ、またはコンテンツの再生若しくはンテンツデータのコピーの回数のデータなどから構成されている。コンテンツデータが利用されると、その利用の形態に対応して、コンテンツ管理データの値は変化する。

【００３６】コンテンツ鍵は、DVDドライブ２のメモリに記憶されている保存鍵で暗号化されている。

【００３７】ネットワーク４は、IEEE1394の規格に基づき、パーソナルコンピュータ１が出力したデータをDVDドライブ２に供給するとともに、DVDドライブ２が出力したデータをパーソナルコンピュータ１に供給する。

【００３８】図２は、パーソナルコンピュータ１の構成を説明するブロック図である。ＣＰＵ（Central Processing Unit）２１は、各種アプリケーションプログラムや、ＯＳ（Operating System）を実際に実行する。ＲＯＭ（Read-only Memory）２２は、一般的には、ＣＰＵ２１が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。ＲＡＭ（Random-Access Memory）２３は、ＣＰＵ２１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはＣＰＵバスまたはメモリバスなどから構成されるホストバス２４により相互に接続されている。

【００３９】ホストバス２４は、ブリッジ２５を介して、ＰＣＩ（Peripheral Component Interconnect/Interface）バスなどの外部バス２６に接続されている。

【００４０】キーボード２８は、ＣＰＵ２１に各種の指令を入力するとき、ユーザにより操作される。マウス２９は、モニタ３０の画面上のポイントの指示や選択を行うとき、ユーザにより操作される。モニタ３０は、液晶表示装置またはＣＲＴ（Cathode Ray Tube）などから成り、各種情報をテキストやイメージで表示する。ＨＤＤ（Hard Disk Drive）３１およびＦＤＤ（Floppy Disk Drive）３２は、それぞれハードディスクまたはフロッピーディスクを駆動し、それらにＣＰＵ２１によって実行するプログラムや情報を記録または再生させる。これらのキーボード２８乃至ＦＤＤ３２は、インターフェース２７に接続されており、インターフェース２７は、外部バス２６、ブリッジ２５、およびホストバス２４を介してＣＰＵ２１に接続されている。

【００４１】IEEE1394インターフェースボード３３は、ネットワーク４が接続され、ＣＰＵ２１、またはＨＤＤ３１から供給されたデータを、IEEE1394に規定されている方式のパケットに格納して、ネットワーク４を介して、送信するとともに、ネットワーク４を介して、受信したパケットに格納されているデータをＣＰＵ２１、またはＨＤＤ３１に出力する。IEEE1394インターフェースボード３３は、また、IEEE1394の規定に基づく所定の処理を実行する。

【００４２】IEEE1394インターフェースボード３３は、外部バス２６、ブリッジ２５、およびホストバス２４を介してＣＰＵ２１に接続されている。

【００４３】次に、図３のブロック図を参照して、DVDドライブ２の構成を説明する。IEEE1394インターフェース５１は、ネットワーク４が接続され、記録再生部５２またはメモリ５３から供給されたデータを、IEEE1394に規定されている方式のパケットに格納して、ネットワーク４を介して、パーソナルコンピュータ１に送信するとともに、ネットワーク４を介して、パーソナルコンピュータ１から受信したパケットに格納されているデータを記録再生部５２またはメモリ５３に出力する。IEEE1394インターフェース５１は、また、IEEE1394の規定に基づく所定の処理を実行する。

【００４４】IEEE1394インターフェース５１は、また、パーソナルコンピュータ１と、後述する相互認証の処理を実行する。IEEE1394インターフェース５１は、相互認証の処理のときのみ、メモリ５３に記憶されているデータを読み出すとともに、メモリ５３に所定のデータを記憶させる。

【００４５】メモリ５３は、物理的に分解されたときに内部の構造をわかりにくくするためのアルミニュウムの層を有し、DVDドライブ２から取り外されたとき、単独で動作させにくくする為に、所定の限られた範囲の電圧でのみ動作するなど耐タンパー性を有する半導体メモリで、保存鍵およびコンテンツ管理データのハッシュ値を記憶している。

【００４６】記録再生部５２は、DVD３が装着され、装着されているDVD３に記録されているコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを読み出してIEEE1394インターフェース５１に出力するとともに、装着されているDVD３にIEEE1394インターフェース５１から供給されたコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを記録させる。

【００４７】図４は、DVDドライブ２に記憶されているデータ、またはDVD３に記録されているデータを説明する図である。DVD３は、保存鍵により暗号化されているコンテンツ鍵、コンテンツ鍵により暗号化されているコンテンツデータ、およびコンテンツデータの利用の形態を管理するためのコンテンツ管理データが記録されている。

【００４８】DVDドライブ２のメモリ５３は、保存鍵、およびコンテンツ管理データに所定のハッシュ関数を適用して得られたハッシュ値を記憶している。DVDドライブ２のメモリ５３に記憶されている保存鍵、またはコンテンツ管理データのハッシュ値は、IEEE1394インターフェース５１がパーソナルコンピュータ１と相互認証するときのみ、メモリ５３から読み出され、または値が更新される。

【００４９】図５は、DVDドライブ２およびパーソナルコンピュータ１が相互認証するとき、ネットワーク４を介して、伝送されるデータの一部を説明する図である。コンテンツデータの利用に伴う相互認証において、パーソナルコンピュータ１は、所定のビット数の乱数（例えば、６４ビット）を生成するとともに、DVDドライブ２から受信した現在のコンテンツ管理データに対して、コンテンツデータの利用に対応する変更を加えて更新し、更新後のコンテンツ管理データを生成する。

【００５０】パーソナルコンピュータ１は、DVDドライブ２から受信したコンテンツ管理データおよび更新したコンテンツ管理データのそれぞれに、ＭＤ５などの一方向ハッシュ関数を適用して、受信したコンテンツ管理データおよび更新したコンテンツ管理データのそれぞれの一方向性暗号値であるハッシュ値を求める。

【００５１】パーソナルコンピュータ１は、生成した乱数、現在のコンテンツ管理データのハッシュ値、および更新後のコンテンツ管理データのハッシュ値を、DVDドライブ２に送信する。

【００５２】パーソナルコンピュータ１が生成した乱数、現在のコンテンツ管理データのハッシュ値、およびパーソナルコンピュータ１が更新したコンテンツ管理データのハッシュ値を受信したDVDドライブ２は、パーソナルコンピュータ１が生成した乱数、現在のコンテンツ管理データ、および更新されたコンテンツ管理データのそれぞれを暗号化する。

【００５３】DVDドライブ２は、暗号化したパーソナルコンピュータ１が生成した乱数、暗号化した現在のコンテンツ管理データのハッシュ値、および暗号化した更新されたコンテンツ管理データのハッシュ値を、パーソナルコンピュータ１に送信する。

【００５４】DVDドライブ２は、所定のビット数の乱数（例えば、６４ビット）を生成して、パーソナルコンピュータ１に送信する。

【００５５】パーソナルコンピュータ１は、DVDドライブ２から送信された所定のビット数の乱数を暗号化して、DVDドライブ２に送信する。

【００５６】次に、本発明に係る記録システムのコンテンツの再生の処理を、図６のフローチャートを参照して説明する。ステップＳ１１において、パーソナルコンピュータ１およびDVDドライブ２は、相互認証して、共通鍵を生成する。相互認証の処理の詳細は、図７のフローチャートを参照して後述する。ステップＳ１２において、DVDドライブ２のIEEE1394インターフェース５１は、メモリ５３に記憶されている保存鍵を読み出し、記録再生部５２に、装着されているDVD３からコンテンツ鍵を読み出させる。メモリ５３に記憶されている保存鍵を読み出す処理は、ステップＳ１１の相互認証の処理で実行してもよい。DVDドライブ２のIEEE1394インターフェース５１は、コンテンツ鍵を保存鍵で復号する。

【００５７】ステップＳ１３において、DVDドライブ２

のIEEE1394インターフェース５１は、ステップＳ１１で生成された共通鍵で、コンテンツ鍵を暗号化する。ステップＳ１４において、DVDドライブ２のIEEE1394インターフェース５１は、ネットワーク４を介して、共通鍵で暗号化されたコンテンツ鍵をパーソナルコンピュータ１に送信する。

【００５８】ステップＳ１５において、パーソナルコンピュータ１のIEEE1394インターフェースボード３３は、ネットワーク４を介して、DVDドライブ２から送信された、共通鍵で暗号化されたコンテンツ鍵を受信する。ステップＳ１６において、DVDドライブ２のIEEE1394インターフェース５１は、記録再生部５２に、装着されているDVD３から、コンテンツ鍵で暗号化されているコンテンツデータを読み出させる。DVDドライブ２のIEEE1394インターフェース５１は、ネットワーク４を介して、コンテンツ鍵で暗号化されているコンテンツデータをパーソナルコンピュータ１に送信する。

【００５９】ステップＳ１７において、パーソナルコンピュータ１のIEEE1394インターフェースボード３３は、DVDドライブ２から送信された、コンテンツ鍵で暗号化されているコンテンツデータを受信する。ステップＳ１８において、パーソナルコンピュータ１のＣＰＵ２１は、ステップＳ１５で受信したコンテンツ鍵を、ステップＳ１１で生成した共通鍵で復号する。

【００６０】ステップＳ１９は、パーソナルコンピュータ１のＣＰＵ２１は、復号したコンテンツ鍵で、ステップＳ１７で受信したコンテンツデータを復号する。

【００６１】ステップＳ２０において、パーソナルコンピュータ１のIEEE1394インターフェースボード３３は、ステップＳ１１の相互認証の処理で更新されたコンテンツ管理データを、ネットワーク４を介して、DVDドライブ２に送信する。ステップＳ２１において、DVDドライブ２のIEEE1394インターフェース５１は、更新されたコンテンツ管理データを、受信する。ステップＳ２２において、DVDドライブ２の記録再生部５２は、装着されているDVD３に更新されたコンテンツ管理データを記録させる。

【００６２】ステップＳ２３において、パーソナルコンピュータ１は、復号したコンテンツデータからコンテンツを再生して、処理は終了する。

【００６３】このように、パーソナルコンピュータ１は、DVDドライブ２からコンテンツ鍵およびコンテンツデータを受信して、コンテンツを再生する。

【００６４】次に、図６のフローチャートのステップＳ１１の処理に対応する、パーソナルコンピュータ１およびDVDドライブ２の相互認証の処理を、図７のフローチャートを参照して説明する。ステップＳ３１において、DVDドライブ２のIEEE1394インターフェース５１は、記録再生部５２に、装着されているDVD３からコンテンツ管理データを読み出させる。IEEE1394インターフェース５１は、ネットワーク４を介して、コンテンツ管理データをパーソナルコンピュータ１に送信する。

【００６５】ステップＳ５１において、パーソナルコンピュータ１のIEEE1394インターフェースボード３３は、ネットワーク４を介して、DVDドライブ２から送信されたコンテンツ管理データを受信する。ステップＳ５２において、パーソナルコンピュータ１のＣＰＵ２１は、DVDドライブ２から受信したコンテンツ管理データにＭＤ５などの一方向ハッシュ関数を適用して、コンテンツ管理データのハッシュ値Ｈａを計算する。

【００６６】ステップＳ５３において、パーソナルコンピュータ１のＣＰＵ２１は、コンテンツの再生に対応させて、コンテンツの再生後のコンテンツ管理データを計算する。ステップＳ５４において、パーソナルコンピュータ１のＣＰＵ２１は、コンテンツの再生後のコンテンツ管理データにＭＤ５などのハッシュ関数を適用して、コンテンツの再生後のコンテンツ管理データのハッシュ値Ｈｂを計算する。

【００６７】ステップＳ５５において、パーソナルコンピュータ１のＣＰＵ２１は、例えば、６４ビットの乱数Ｒａを生成する。ステップＳ５６において、パーソナルコンピュータ１のIEEE1394インターフェースボード３３は、ネットワーク４を介して、DVDドライブ２に、乱数Ｒａ、ハッシュ値Ｈａ、およびハッシュ値Ｈｂを送信する。

【００６８】ステップＳ３２において、DVDドライブ２のIEEE1394インターフェース５１は、パーソナルコンピュータ１から送信された乱数Ｒａ、ハッシュ値Ｈａ、およびハッシュ値Ｈｂを受信する。ステップＳ３３において、DVDドライブ２のIEEE1394インターフェース５１は、メモリ５３に記憶されているコンテンツ管理データのハッシュ値と、ステップＳ３２で受信したハッシュ値Ｈａとが一致するか否かを判定し、メモリ５３に記憶されているコンテンツ管理データのハッシュ値と、ステップＳ３２で受信したハッシュ値Ｈａとが一致しないと判定された場合、コンテンツ管理データに改竄があったので、相互認証しないで、処理は終了する。

【００６９】ステップＳ３３において、メモリ５３に記憶されているコンテンツ管理データのハッシュ値と、ステップＳ３２で受信したハッシュ値Ｈａとが一致すると判定された場合、コンテンツ管理データに改竄がなかったので、ステップＳ３４に進み、DVDドライブ２のIEEE1394インターフェース５１は、ステップＳ３２で受信した乱数Ｒａ、ハッシュ値Ｈａ、およびハッシュ値Ｈｂを暗号化する。

【００７０】ステップＳ３５において、DVDドライブ２のIEEE1394インターフェース５１は、ネットワーク４を介して、暗号化した乱数Ｒａ、暗号化したハッシュ値Ｈａ、および暗号化したハッシュ値Ｈｂをパーソナルコンピュータ１に送信する。

【００７１】ステップＳ５７において、パーソナルコンピュータ１のＣＰＵ２１は、乱数Ｒａ、ハッシュ値Ｈａ、およびハッシュ値Ｈｂを暗号化する。

【００７２】パーソナルコンピュータ１およびDVDドライブ２が共に正当である場合、ステップＳ３４におけるDVDドライブ２のIEEE1394インターフェース５１の暗号化の方式および暗号鍵は、ステップＳ５７におけるパーソナルコンピュータ１のＣＰＵ２１の暗号化の方式および暗号鍵と、それぞれ同一であり、パーソナルコンピュータ１およびDVDドライブ２において、同一の暗号化した乱数Ｒａ、暗号化したハッシュ値Ｈａ、および暗号化したハッシュ値Ｈｂが得られる。

【００７３】ステップＳ５８において、パーソナルコンピュータ１のIEEE1394インターフェースボード３３は、ネットワーク４を介して、DVDドライブ２から送信された暗号化された乱数Ｒａ、暗号化されたハッシュ値Ｈａ、および暗号化されたハッシュ値Ｈｂを受信する。ステップＳ５９において、パーソナルコンピュータ１のＣＰＵ２１は、ステップＳ５７で暗号化した乱数Ｒａ、暗号化したハッシュ値Ｈａ、および暗号化したハッシュ値Ｈｂのそれぞれと、ステップＳ５８で受信した暗号化された乱数Ｒａ、暗号化されたハッシュ値Ｈａ、および暗号化されたハッシュ値Ｈｂのそれぞれとを比較して一致するか否かを判定し、暗号化した乱数Ｒａ、暗号化したハッシュ値Ｈａ、および暗号化したハッシュ値Ｈｂのそれぞれと、受信した暗号化された乱数Ｒａ、暗号化されたハッシュ値Ｈａ、および暗号化されたハッシュ値Ｈｂのいずれかが一致しないと判定された場合、DVDドライブ２は正当ではないので、DVDドライブ２を認証せず、処理は終了する。

【００７４】ステップＳ３６において、DVDドライブ２のIEEE1394インターフェース５１は、６４ビットの乱数Ｒｂを生成する。ステップＳ３７において、DVDドライブ２のIEEE1394インターフェース５１は、ネットワーク４を介して、生成した乱数Ｒｂをパーソナルコンピュータ１に送信する。ステップＳ３８において、DVDドライブ２のIEEE1394インターフェース５１は、乱数Ｒｂを暗号化する。

【００７５】ステップＳ５９において、暗号化した乱数Ｒａ、ハッシュ値Ｈａ、およびハッシュ値Ｈｂのそれぞれと、受信した暗号化された乱数Ｒａ、ハッシュ値Ｈａ、およびハッシュ値Ｈｂそれぞれとが一致すると判定された場合、DVDドライブ２は正当なので、ステップＳ６０に進み、パーソナルコンピュータ１のIEEE1394インターフェースボード３３は、ネットワーク４を介して、DVDドライブ２が送信した乱数Ｒｂを受信する。

【００７６】ステップＳ６１において、パーソナルコンピュータ１のＣＰＵ２１は、ステップＳ６０で受信した乱数Ｒｂを暗号化する。パーソナルコンピュータ１およびDVDドライブ２が正当である場合、ステップＳ３８におけるDVDドライブ２のIEEE1394インターフェース５１の暗号化の方式および暗号鍵は、ステップＳ６１におけるパーソナルコンピュータ１のＣＰＵ２１の暗号化の方式および暗号鍵と、それぞれ同一であるので、暗号化された乱数の値は同一となる。

【００７７】ステップＳ６２において、パーソナルコンピュータ１のIEEE1394インターフェースボード３３は、ネットワーク４を介して、ステップＳ６１で暗号化した乱数ＲｂをDVDドライブ２に送信する。

【００７８】ステップＳ３９において、DVDドライブ２のIEEE1394インターフェース５１は、ネットワーク４を介して、パーソナルコンピュータ１が送信した暗号化された乱数Ｒｂを受信する。ステップＳ４０において、DVDドライブ２のIEEE1394インターフェース５１は、ステップＳ３８で暗号化した乱数Ｒｂとステップ３９で受信した暗号化された乱数Ｒｂとが一致するか否かを判定し、ステップＳ３８で暗号化した乱数Ｒｂとステップ３９で受信した暗号化された乱数Ｒｂとが一致しないと判定された場合、パーソナルコンピュータ１が正当ではないので、パーソナルコンピュータ１を認証しないで、処理は終了する。

【００７９】ステップＳ４０において、ステップＳ３８で暗号化した乱数Ｒｂとステップ３９で受信した暗号化された乱数Ｒｂとが一致すると判定された場合、パーソナルコンピュータ１が正当なので、ステップＳ４１に進み、DVDドライブ２のIEEE1394インターフェース５１は、メモリ５３に、ステップＳ３２で受信したハッシュ値Ｈｂを記憶させる。

【００８０】ステップＳ４２において、DVDドライブ２のIEEE1394インターフェース５１は、パーソナルコンピュータ１を認証したので、乱数Ｒａおよび乱数Ｒｂから共通鍵を生成し、DVDドライブ２の処理は終了する。

【００８１】ステップＳ６３において、パーソナルコンピュータ１のＣＰＵ２１は、DVDドライブ２を認証したので、乱数Ｒａおよび乱数Ｒｂから共通鍵を生成し、パーソナルコンピュータ１の処理は終了する。

【００８２】このように、DVDドライブ２は、コンテンツ管理データのハッシュ値をメモリ５３に記憶して、相互認証の手続きで、パーソナルコンピュータ１が計算したハッシュ値と比較するので、コンテンツ管理データが改竄されたとき、パーソナルコンピュータ１を認証しない。

【００８３】DVDドライブ２は、相互認証の手続きで、受信した新たなコンテンツ管理データのハッシュ値を耐タンパ性を有するメモリ５３に記憶するので、新たなコンテンツ管理データのハッシュ値の改竄が防止される。

【００８４】パーソナルコンピュータ１は、その都度生成した乱数とともに、コンテンツ管理データのハッシュ値をDVDドライブ２に送信するので、パーソナルコンピュータ１になりすました機器が、コンテンツ管理データ

のハッシュ値を受信して記憶し、相互認証しようとしても、相互認証は成功しない。

【００８５】なお、コンテンツデータの再生の回数が制限されていない場合など、ステップＳ５３で計算されるコンテンツの再生後のコンテンツ管理データは、ステップＳ５１で受信したコンテンツ管理データと同一でもよい。

【００８６】次に、記録媒体に記録されているコンテンツデータを不正なコピーを防止しつつ、他の記録媒体に移動させることができる、他の記録システムについて説明する。図８は、コンテンツデータを移動することができる、記録システムの他の実施の形態を示す図である。パーソナルコンピュータ１０１は、SCSI (Small Computer System Interface) を介して、MO (Magneto-Optical disk) ドライブ１０２およびハードディスク装置１０４に接続されている。

【００８７】MOドライブ１０２は、装着されているＭＯ１０３に記録されている音声または画像のデータであるコンテンツデータを読み出し、パーソナルコンピュータ１０１または、ハードディスク装置１０４に供給する。MOドライブ１０２は、後述するメモリに、ＭＯ１０３に記録されているコンテンツ鍵を暗号化する暗号鍵である保存鍵、およびコンテンツ管理データにMD５などの一方向ハッシュ関数を適用して得られた値であるハッシュ値を記憶している。

【００８８】ＭＯ１０３は、暗号化されているコンテンツデータ、コンテンツデータを暗号化している暗号鍵であるコンテンツ鍵、およびコンテンツデータの利用を管理するためのコンテンツ管理データを記録している。

【００８９】ＭＯ１０３に記録されているコンテンツデータは、共通鍵暗号方式であるDESまたはIDEAなどの方式で、コンテンツ鍵で暗号化されている。

【００９０】ＭＯ１０３に記録されているコンテンツデータは、コンテンツ管理データに基づき、再生回数、他の記録媒体へのコピー、他の記録媒体への移動が管理され、これらの操作が許可される。

【００９１】コンテンツ管理データは、コンテンツデータが許可されている利用の形態を示すデータ、またはコンテンツの再生若しくはンテンツデータのコピーの回数のデータなどから構成されている。コンテンツデータが利用されると、その利用の形態に対応して、コンテンツ管理データの値は変化する。

【００９２】コンテンツ鍵は、MOドライブ１０２のメモリに記憶されている保存鍵で暗号化されている。

【００９３】ハードディスク装置１０４は、内蔵されているハードディスクドライブにパーソナルコンピュータ１０１またはMOドライブ１０２から供給されたデータを記録するとともに、記録されているデータをパーソナルコンピュータ１０１またはMOドライブ１０２に供給する。

【００９４】図９は、パーソナルコンピュータ１０１の構成を説明するブロック図である。ＣＰＵ１２１乃至ＦＤＤ１３２のそれぞれは、それぞれ図２のＣＰＵ２１乃至ＦＤＤ３２と同様であるので、その説明は省略する。

【００９５】SCSIインターフェースボード１３３は、所定のSCSIケーブルが接続され、ＣＰＵ２１、ＲＡＭ１２３、またはＨＤＤ３１から供給されたデータを、MOドライブ１０２またはハードディスク装置１０４に送信するとともに、MOドライブ１０２またはハードディスク装置１０４から受信したデータをＣＰＵ２１、ＲＡＭ１２３、またはＨＤＤ３１に出力する。

【００９６】SCSIインターフェースボード１３３は、外部バス１２６、ブリッジ１２５、およびホストバス１２４を介してＣＰＵ１２１に接続されている。

【００９７】次に、図１０のブロック図を参照して、ＭＯドライブ１０２の構成を説明する。SCSIインターフェース１５１は、SCSIケーブルが接続され、記録再生部１５２またはメモリ１５３から供給されたデータを、パーソナルコンピュータ１０１またはハードディスク装置１０４に送信するとともに、パーソナルコンピュータ１０１またはハードディスク装置１０４から受信したデータを記録再生部１５２またはメモリ１５３に出力する。

【００９８】SCSIインターフェース１５１は、パーソナルコンピュータ１０１またはハードディスク装置１０４と、図７のフローチャートを参照して説明した相互認証の処理を実行する。SCSIインターフェース１５１は、相互認証の処理のときのみ、メモリ１５３に記憶されているデータを読み出すとともに、メモリ１５３に所定のデータを記憶させる。

【００９９】メモリ１５３は、物理的に分解されたときに内部の構造をわかりにくくするためのアルミニュウムの層を有し、ＭＯドライブ１０２から取り外されたとき、単独で動作させにくくする為に、所定の限られた範囲の電圧でのみ動作するなど耐タンパー性を有する半導体メモリで、保存鍵およびコンテンツ管理データのハッシュ値を記憶している。

【０１００】記録再生部１５２は、ＭＯ１０２が装着され、装着されているＭＯ１０２に記録されているコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを読み出してSCSIインターフェース１５１に出力するとともに、装着されているＭＯ１０２にSCSIインターフェース１５１から供給されたコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを記録させる。

【０１０１】次に、図１１のブロック図を参照して、ハードディスク装置１０４の構成を説明する。SCSIインターフェース１６１は、SCSIケーブルが接続され、ハードディスクドライブ１６２またはメモリ１６３から供給されたデータを、パーソナルコンピュータ１０１またはＭＯドライブ１０２に送信するとともに、パーソナルコン

ピュータ１０１またはMOドライブ１０２から受信したデータをハードディスクドライブ１６２またはメモリ１６３に出力する。

【０１０２】SCSIインターフェース１６１は、パーソナルコンピュータ１０１またはMOドライブ１０２と、図７のフローチャートを参照して説明した相互認証の処理を実行する。SCSIインターフェース１６１は、相互認証の処理のときのみ、メモリ１６３に記憶されているデータを読み出すとともに、メモリ１６３に所定のデータを記憶させる。

【０１０３】メモリ１６３は、物理的に分解されたときに内部の構造をわかりにくくするためのアルミニュウムの層を有し、ハードディスク装置１０４から取り外されたとき、単独で動作させにくくする為に、所定の限られた範囲の電圧でのみ動作するなど耐タンパー性を有する半導体メモリで、保存鍵およびコンテンツ管理データのハッシュ値を記憶している。

【０１０４】ハードディスクドライブ１６２は、内蔵されているハードディスクに記録されているコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを読み出してSCSIインターフェース１６１に出力するとともに、内蔵されているハードディスクにSCSIインターフェース１６１から供給されたコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを記録させる。

【０１０５】図１２は、図８に示す記録システムの、MOドライブ１０２に装着されているMO１０３に記録されているコンテンツデータを、ハードディスクドライブ１６２に移動する処理を説明するフローチャートである。ステップＳ８１において、MOドライブ１０２の記録再生部１５２は、MO１０３に記憶されているコンテンツ管理データを基に、移動後のコンテンツ管理データを計算する。記録再生部１５２は、計算した移動後のコンテンツ管理データをSCSIインターフェース１５１に供給する。

【０１０６】ステップＳ８２において、MOドライブ１０２のSCSIインターフェース１５１およびパーソナルコンピュータ１０１のSCSIインターフェースボード１３３は、図７のフローチャートを参照して説明した処理と同様の手続きで、相互認証して、共通鍵Ｋ１を生成する。

【０１０７】ただし、ステップＳ３１において、SCSIインターフェースボード１３３は、パーソナルコンピュータ１０１に現在のコンテンツ管理データおよび移動後のコンテンツ管理データを送信し、パーソナルコンピュータ１０１は、受信した現在のコンテンツ管理データおよび移動後のコンテンツ管理データを基に、ハッシュ値を計算する。

【０１０８】ステップＳ８３において、MOドライブ１０２のSCSIインターフェース１５１は、ステップＳ８２の相互認証と同時に、メモリ１５３に記憶されているコンテンツ管理データをステップＳ８１で計算した移動後の値に変更させる。

【０１０９】ステップＳ８４において、MOドライブ１０２のSCSIインターフェース１５１は、記録再生部１５２にMO１０３からコンテンツ鍵を読み出させ、メモリ１５３に記憶されている保存鍵でコンテンツ鍵を復号する。

【０１１０】ステップＳ８５において、MOドライブ１０２のSCSIインターフェース１５１は、復号されたコンテンツ鍵をステップＳ８２で生成した共通鍵Ｋ１で暗号化する。ステップＳ８６において、MOドライブ１０２のSCSIインターフェース１５１は、共通鍵Ｋ１で暗号化されたコンテンツ鍵を、パーソナルコンピュータ１０１に送信する。

【０１１１】ステップＳ８７において、パーソナルコンピュータ１０１のSCSIインターフェースボード１３３は、MOドライブ１０２から送信された暗号化されているコンテンツ鍵を受信する。

【０１１２】ステップＳ８８において、パーソナルコンピュータ１０１のＣＰＵ１２１は、ステップＳ８７で受信したコンテンツ鍵を、ステップＳ８２で生成した共通鍵Ｋ１で復号する。

【０１１３】ステップＳ８９において、ハードディスク装置１０４のハードディスクドライブ１６２は、移動後のコンテンツ管理データ（相互認証の処理に利用される）を計算する。

【０１１４】ステップＳ９０において、ハードディスク装置１０４のSCSIインターフェース１６１およびパーソナルコンピュータ１０１のSCSIインターフェースボード１３３は、図７のフローチャートを参照して説明した処理と同様の手続きで、相互認証して、共通鍵Ｋ２を生成する。ステップＳ９０のパーソナルコンピュータ１０１とハードディスク装置１０４の相互認証の処理で、パーソナルコンピュータ１０１は、ハードディスク装置１０４にステップＳ８１でMOドライブ１０２が計算した移動後のコンテンツ管理データを送信する。

【０１１５】ステップＳ９１において、ハードディスク装置１０４のSCSIインターフェース１６１は、ステップＳ９０の相互認証と同時に、メモリ１６３に記憶されているコンテンツ管理データを、ステップＳ９０で受信した移動後のコンテンツ管理データに変更させる。

【０１１６】ステップＳ９２において、パーソナルコンピュータ１０１のＣＰＵ１２１は、ステップＳ８８で復号されたコンテンツ鍵を、共通鍵Ｋ２で暗号化する。ステップＳ９３において、パーソナルコンピュータ１０１のSCSIインターフェースボード１３３は、共通鍵Ｋ２で暗号化されているコンテンツ鍵をハードディスク装置１０４に送信する。

【０１１７】ステップＳ９４において、ハードディスク装置１０４のSCSIインターフェース１６１は、パーソナ

ルコンピュータ１０１から送信された、共通鍵Ｋ２で暗号化されているコンテンツ鍵を受信する。

【０１１８】ステップＳ９５において、ハードディスク装置１０４のSCSIインターフェース１６１は、ステップＳ９４で受信したコンテンツ鍵を共通鍵Ｋ２で復号する。

【０１１９】ステップＳ９６において、MOドライブ１０２の記録再生部１５２は、装着されているMO１０３からコンテンツ鍵を削除する。

【０１２０】ステップＳ９７において、ハードディスク装置１０４のSCSIインターフェース１６１は、ステップＳ９５で復号されたコンテンツ鍵を、メモリ１６３に記憶している保存鍵で暗号化する。ステップＳ９８において、ハードディスク装置１０４のハードディスクドライブ１６２は、暗号化されたコンテンツ鍵を記録する。

【０１２１】ステップＳ９９において、MOドライブ１０２のSCSIインターフェース１５１は、記録再生部１５２にMO１０３からコンテンツデータを読み出させ、ハードディスク装置１０４にコンテンツデータを移動する。

【０１２２】このように、図８に示す記録システムにおいては、MO１０３に記録されているコンテンツデータをハードディスク装置１０４に移動する。MO１０３に記録されているコンテンツデータを他のMOディスクにバックアップしておき、MO１０３に記録されているコンテンツデータを利用した後、バックアップされたコンテンツデータが記録されているMOディスクを使用しようとしても、ステップＳ８２の相互認証の処理で不正と判定されるので、バックアップしたコンテンツデータを使用することができない。

【０１２３】なお、コンテンツデータが記録される記録媒体は、DVD３、MO１０３、またはハードディスクとして説明したが、光ディスク、半導体メモリ、磁気テープ、または印刷物（例えば、２次元バーコードが印刷された印刷物）でもよい。

【０１２４】また、記録媒体に記録するコンテンツデータは、音声または画像（動画像または静止画像）として説明したが、コンピュータプログラム、所定のサーバなどへのアクセス権を記述したデータ（ファイル）、または所定のサービスを利用するためのデータを記憶したチケットなどでもよい。

【０１２５】コンテンツを再生する装置は、パーソナルコンピュータ１またはパーソナルコンピュータ１０１として説明したが、パーソナルコンピュータ１またはパーソナルコンピュータ１０１に限らず、セットトップボックスなどの家庭電化製品、サーバ、またはDVDドライブなどのコンピュータ周辺装置などでもよい。

【０１２６】パーソナルコンピュータ１またはパーソナルコンピュータ１０１が実行するコンテンツの再生の処理、相互認証の処理などのプログラムを内部が解析しにくいソフトウェアとすれば、コンテンツデータの不正使用に対する防御をより強力にすることができる。

【０１２７】パーソナルコンピュータ１、パーソナルコンピュータ１０１、DVDドライブ２、MOドライブ１０２、またはハードディスク装置１０４は、IEEE1394の規格に基づくネットワーク４またはSCSIケーブルを介してデータを送信するとともに、受信すると説明したが、他のネットワーク、他のデータ転送用のインターフェースなどでもよい。

【０１２８】例えば、半導体メモリが内蔵された、シリアル制御されるメモリカードは、コンテンツデータである、暗号化した音楽データを記憶している。音楽を再生するとき、メモリカードは、所定のパーソナルコンピュータのインターフェースに装着される。

【０１２９】音楽の再生の回数を制限するため、そのメモリカードに記憶されているコンテンツ管理データは、音楽の再生の回数に対応してデクリメントされる。コンテンツ管理データが”０”になったとき、メモリカードが装着されているパーソナルコンピュータは、メモリカードに記憶されている音楽データを利用しない（音楽を再生しない）。

【０１３０】メモリカードが装着されるインターフェースが、コンテンツ管理データのハッシュ値を記憶すれば、メモリカードに記憶されているコンテンツ管理データを他のメモリカードにバックアップしても、その後に、一度でもメモリカードに記憶されている音楽データが利用されれば、バックアップされた音楽データを再生することはできない。

【０１３１】例えば、メモリカードが装着されるインターフェースが相互認証の処理の際に出力する信号を監視して、その信号を記録し、またその信号を改竄しても、コンテンツ管理データのハッシュ値は、その都度生成された乱数とともに、送信されるので、相互認証を成功させることは、不可能である。

【０１３２】このように、コンテンツデータが記録される記録媒体の種類、信号が送信される方式、インターフェースの種類などに拘わらず、不正な複製を防止することができる。

【０１３３】なお、メモリ５３、メモリ１５３、またはメモリ１６３は、コンテンツ管理データにハッシュ関数を適用して得られるハッシュ値を記憶するとして説明したが、ハッシュ値に限らず、ＤＥＳなどの共通鍵暗号方式で暗号化したコンテンツ管理データを記憶してもよい。

【０１３４】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールす

ることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【０１３５】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図１３に示すように、磁気ディスク３５１（フロッピディスクを含む）、光ディスク３５２（CD-ROM(CompactDisc-Read Only Memory)、ＤＶＤ(Digital Versatile Disc)を含む）、光磁気ディスク３５３（MD(Mini-Disc)を含む）、若しくは半導体メモリ３５４などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM３０２や、記憶部３０８を構成するハードディスクなどにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じてルータ、モデムなどのインタフェースを介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【０１３６】なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０１３７】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０１３８】

【発明の効果】請求項１に記載の送信装置、請求項４に記載の送信方法、および請求項５に記載のプログラム格納媒体によれば、第２のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第２のデータが送信されるとともに、受信装置から第２のデータの暗号値が受信され、受信装置を認証する場合、受信した第２のデータの暗号値と、記憶している第２のデータの暗号値との一致が判定されるようにしたので、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようになる。

【０１３９】請求項６に記載の受信装置、請求項９に記載の受信方法、および請求項１０に記載のプログラム格納媒体によれば、送信装置を認証する場合、送信装置から第１のデータの利用の制限を記述する第２のデータが受信されるとともに、送信装置に第２のデータの暗号値が送信され、送信装置を認証する場合、受信した第２のデータを基に、第２のデータの暗号値が生成されるようにしたので、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようになる。

【０１４０】請求項１１に記載の通信システムによれば、第２のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第２のデータが送信されるとともに、受信装置から第２のデータの暗号値が受信され、受信装置を認証する場合、受信した第２のデータの暗号値と、記憶している第２のデータの暗号値との一致が判定され、送信装置を認証する場合、送信装置から第２のデータが受信されるとともに、送信装置に第２のデータの暗号値が送信され、送信装置を認証する場合、受信した第２のデータを基に、第２のデータの暗号値が生成されるようにしたので、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようになる。

【図面の簡単な説明】

【図１】本発明に係る記録システムの一実施の形態を示す図である。

【図２】パーソナルコンピュータ１の構成を説明するブロック図である。

【図３】DVDドライブ２の構成を説明するブロック図である。

【図４】DVDドライブ２に記憶されているデータ、またはDVD３に記録されているデータを説明する図である。

【図５】DVDドライブ２およびパーソナルコンピュータ１が相互認証するとき、ネットワーク４を介して、送信されるデータの一部を説明する図である。

【図６】コンテンツの再生の処理を説明するフローチャートである。

【図７】相互認証の処理を説明するフローチャートである。

【図８】記録システムの他の実施の形態を示す図である。

【図９】パーソナルコンピュータ１０１の構成を説明するブロック図である。

【図１０】MOドライブ１０２の構成を説明するブロック図である。

【図１１】ハードディスク装置１０４の構成を説明するブロック図である。

【図１２】コンテンツの移動の処理を説明するフローチャートである。

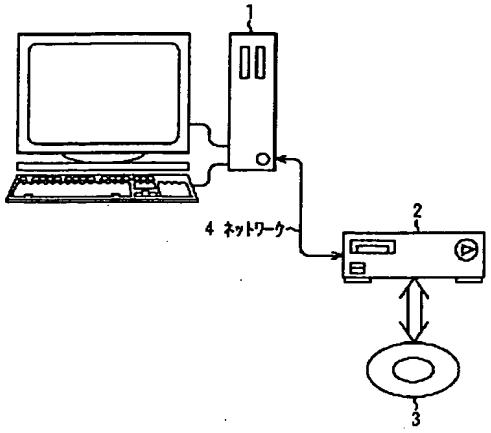
【図１３】プログラム格納媒体を説明する図である。

【符号の説明】

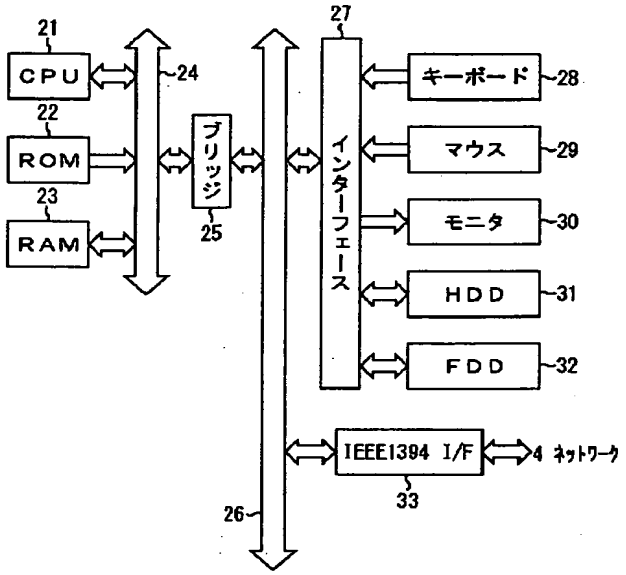
１ パーソナルコンピュータ，２ DVDドライブ，３ DVD，４ ネットワーク，２１ ＣＰＵ，３３ IEEE1394インターフェースボード，５１IEEE1394インターフェース，５２ 記録再生部，５３ メモリ，１０１パーソナルコンピュータ，１０２ MOドライブ，１０３ MO，１０４ハードディスク装置，１２１ ＣＰＵ，１３３ SCSIインターフェースボード，１５１ SCSIインターフェース，１５２ 記録再生部，１５３ メモリ，１６１ SCSIインターフェース，１６２ ハードディスクドライブ，１６３ メモリ，３０１ ＣＰＵ，３０２ ＲＯＭ，３０３ ＲＡＭ，３０８ 記憶部，３５１ 磁気デ

ィスク，　３５２　光ディスク，　３５３光磁気ディス　　ク，　３５４　半導体メモリ

【図１】

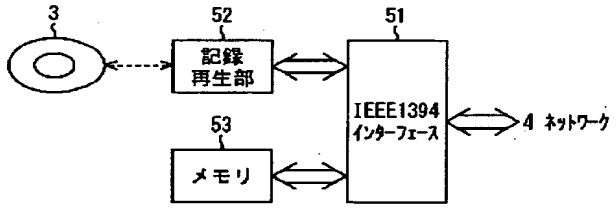


【図２】

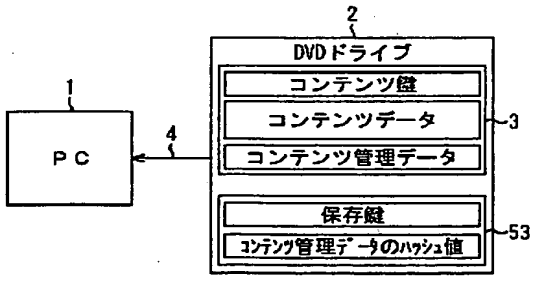


パーソナルコンピュータ 1

【図３】

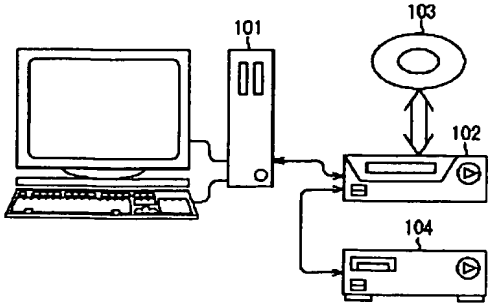


【図４】

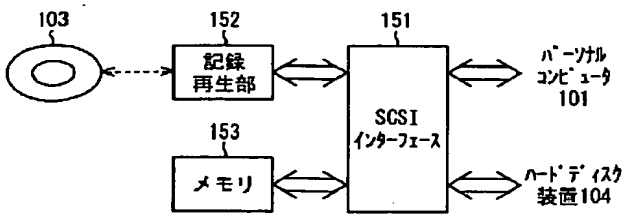


DVDドライブ 2

【図８】

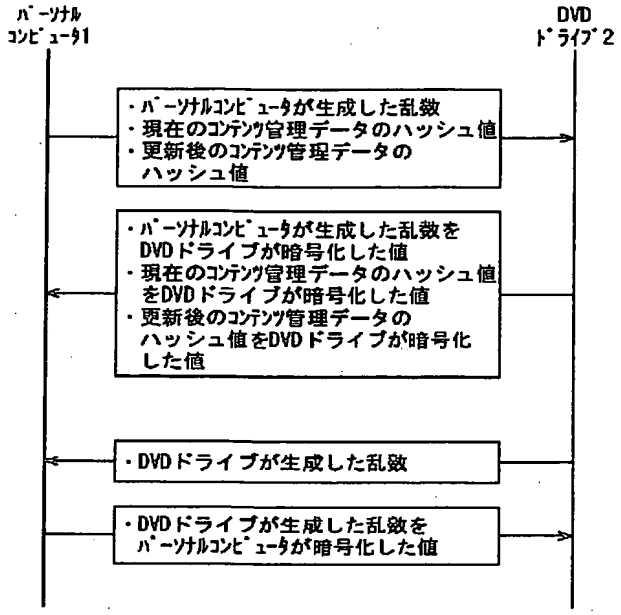


【図１０】

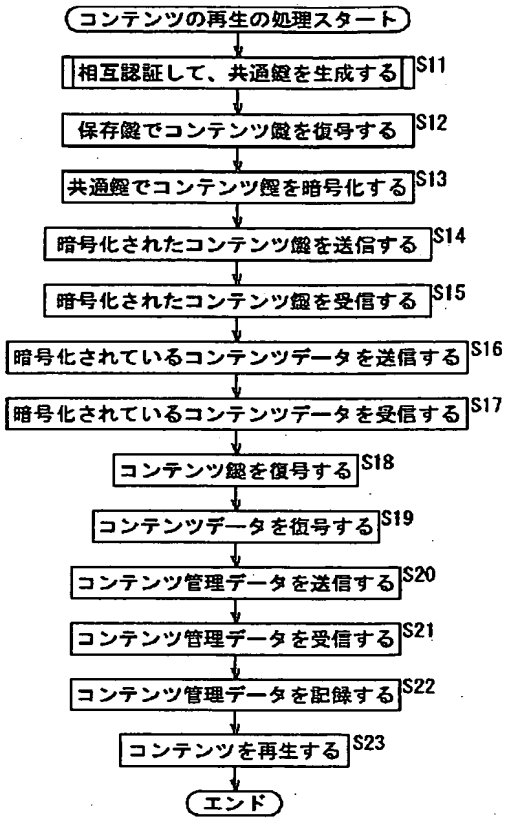


MOドライブ 102

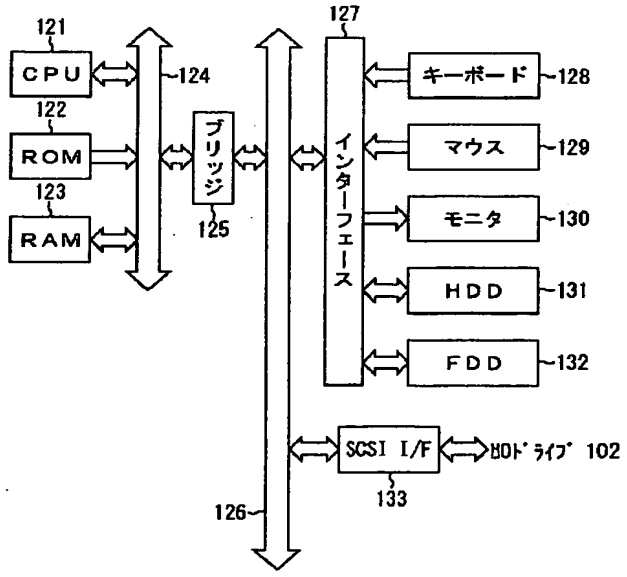
【図５】



【図６】

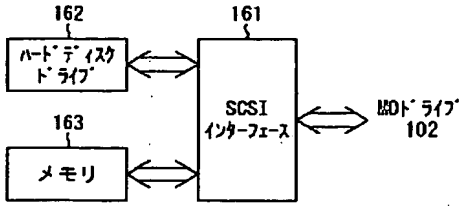


【図９】



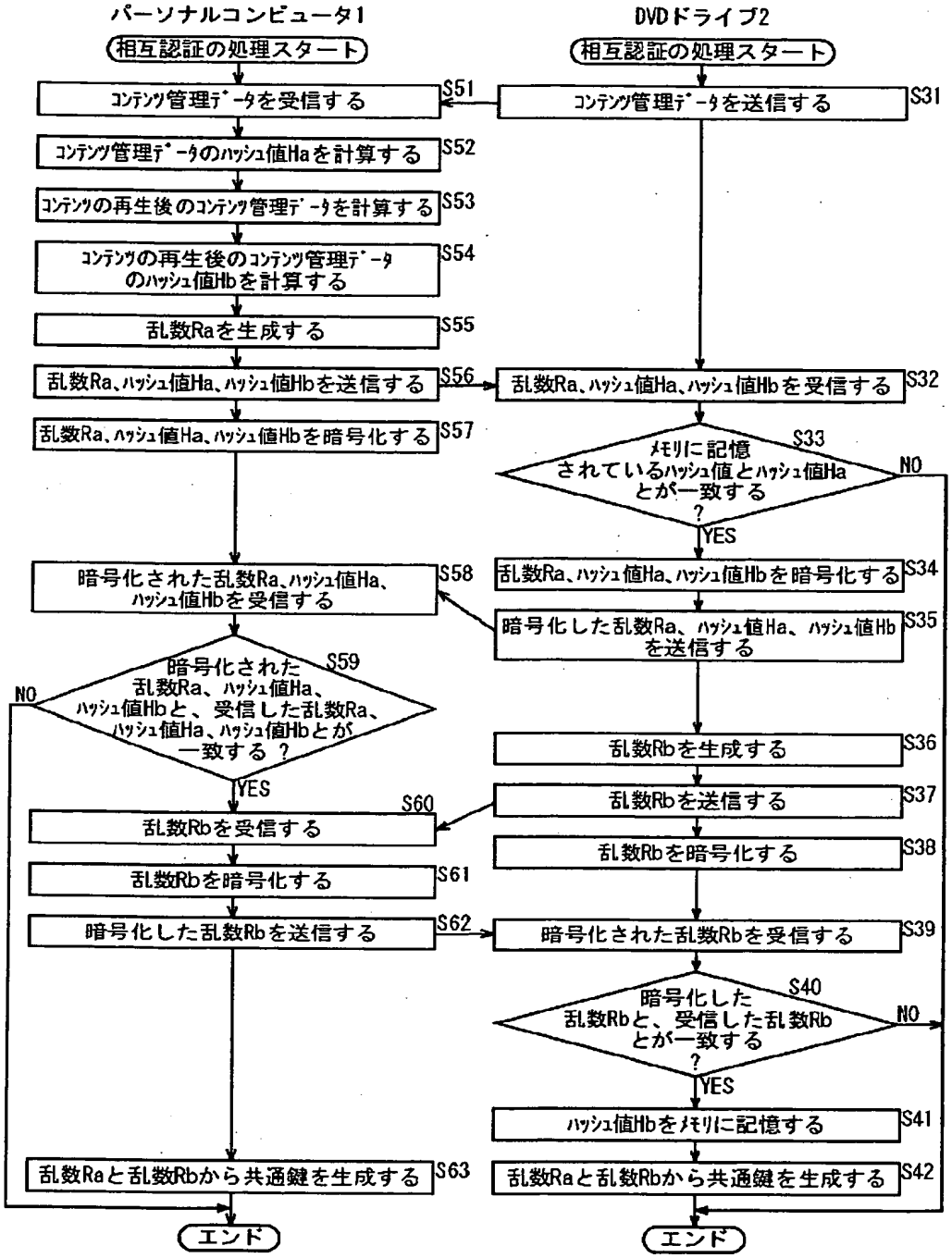
パーソナルコンピュータ 101

【図１１】

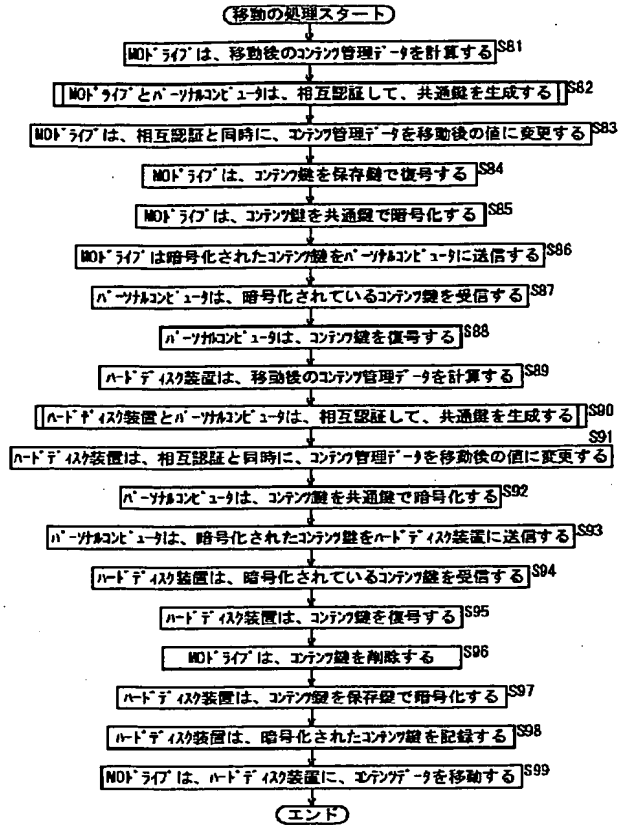


ハードディスク装置 104

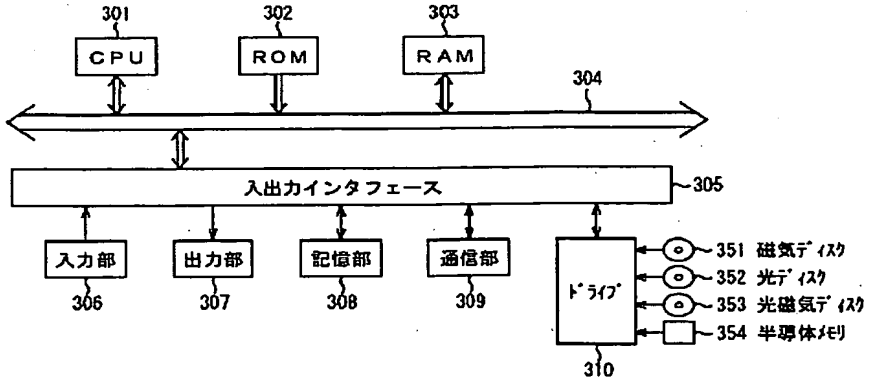
【図７】


パーソナルコンピュータ1
DVDドライブ2
相互認証の処理スタート
相互認証の処理スタート
コンテンツ管理データを受信する
S51
コンテンツ管理データを送信する
S31
コンテンツ管理データのハッシュ値Haを計算する
S52
コンテンツの再生後のコンテンツ管理データを計算する
S53
コンテンツの再生後のコンテンツ管理データのハッシュ値Hbを計算する
S54
乱数Raを生成する
S55
乱数Ra、ハッシュ値Ha、ハッシュ値Hbを送信する
S56
乱数Ra、ハッシュ値Ha、ハッシュ値Hbを受信する
S32
乱数Ra、ハッシュ値Ha、ハッシュ値Hbを暗号化する
S57
メモリに記憶されているハッシュ値とハッシュ値Haとが一致する？
S33
NO
YES
暗号化された乱数Ra、ハッシュ値Ha、ハッシュ値Hbを受信する
S58
乱数Ra、ハッシュ値Ha、ハッシュ値Hbを暗号化する
S34
暗号化した乱数Ra、ハッシュ値Ha、ハッシュ値Hbを送信する
S35
暗号化された乱数Ra、ハッシュ値Ha、ハッシュ値Hbと、受信した乱数Ra、ハッシュ値Ha、ハッシュ値Hbとが一致する？
S59
NO
YES
乱数Rbを生成する
S36
乱数Rbを送信する
S37
乱数Rbを受信する
S60
乱数Rbを暗号化する
S38
乱数Rbを暗号化する
S61
暗号化した乱数Rbを送信する
S62
暗号化された乱数Rbを受信する
S39
暗号化した乱数Rbと、受信した乱数Rbとが一致する？
S40
NO
YES
ハッシュ値Hbをメモリに記憶する
S41
乱数Raと乱数Rbから共通鍵を生成する
S63
乱数Raと乱数Rbから共通鍵を生成する
S42
エンド
エンド

【図１２】



【図１３】



パーソナルコンピュータ 1

フロントページの続き

(51) Int. Cl.[7]	識別記号	FI	テーマコード(参考)
H04L 29/10		H04L 13/00	309C

Fターム(参考) 5B049 AA05 BB11 CC05 CC08 DD01
DD05 EE03 FF03 FF04 FF09
GG04 GG07 GG10
5J104 AA13 FA07 JA01 KA06 NA02
NA12 NA27 NA31 NA32 PA04
PA07
5K032 AA08 DB19
5K034 BB03 DD02 HH01
9A001 EE03 GG22 HH15 JJ19 KK43
KK62 LL03